4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 130 500 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.09.2001 Bulletin 2001/36

(51) Int Cl.7: G06F 1/00

(21) Application number: 01300144.1

(22) Date of filing: 09.01.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 20.01.2000 JP 2000014195

(71) Applicant: SONY CORPORATION
Tokyo 141 (JP)

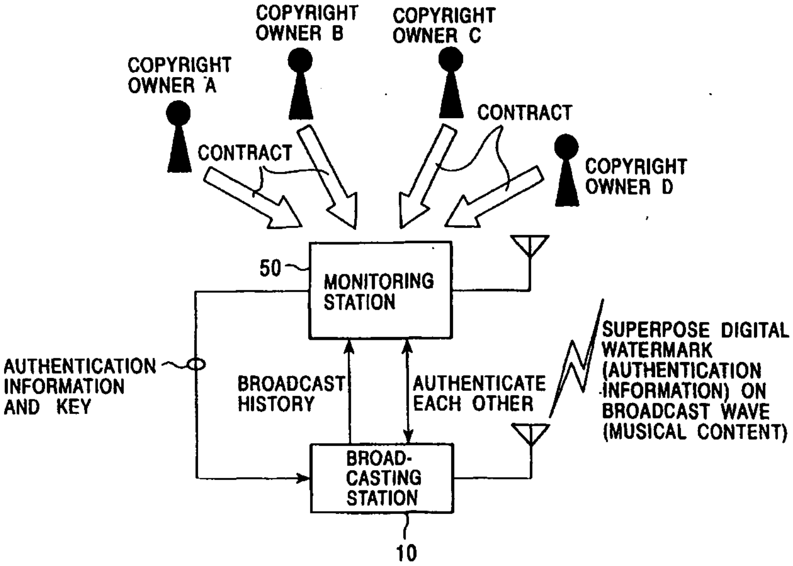
(72) Inventor: Hirai, Jun,
Intellectual Property Department
Tokyo 141 (JP)

(74) Representative: Turner, James Arthur et al
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) System and method for distribution and monitoring of copyrighted data

(57) In order to appropriately manage or monitor a content distribution status and to accurately impose a content royalty, a content distribution system includes a monitoring apparatus for issuing authentication information showing a content-use consent and monitoring the distribution of a content, and a distribution apparatus for distributing the content via a predetermined distribution path with the attached authentication information. The monitoring apparatus, in which the authentication information is composed of the set of time identification information showing the current time and distributor identification information assigned to the distribution apparatus, obtains a content being distributed in the distribution path, and can determine the validity of the distributed content on the basis of whether or not the authentication information is attached to the content.

FIG. 2



Printed by Jouve, 75001 PARIS (FR)

Description

[0001] This invention relates to content distribution systems, content distribution methods, content distribution status monitoring apparatus and methods and content disbributed using such apparatus and methods.

[0002] A copyright is a relatively exclusive property right capable of being used for authored material and is contained in one of commonly called "intangible property rights". The "authored material" referred to herein are ones in which thoughts or feelings are expressed in a creative manner and refers to ones which belong to the fields of the arts, sciences, fine arts, or music. A copyright is protected by, for example, copyright acts by individual countries and by international treaties such as the Berne Convention or the Universal Copyright Convention.

[0003] It is quite rare for a copyright to be asserted by the copyright owner himself, and it is usual for the copyright owner to obtain a fixed amount of payment for the use of the copyright by another person, and consents to the use of the copyright. For example, a record company having copyrights on music content such as musical pieces can demand, with respect to a broadcasting station which uses, that is, broadcasts, music content and to content distribution dealers, copyright royalty corresponding to the number of times the content is used.

[0004] In recent years, information processing and information communication technologies have made rapid progress, and internationalization has advanced remarkably in the cultural and economical fields. In such a social environment, the situation concerning copyrights is constantly changing. It is said that the history of copyright protection dates from the invention of printing technology at around the middle of the fifteenth century. At the present time, all data and content are being digitized, so that they can be handled on computer systems, and as a consequence of this, duplication of copyrighted material is becoming progressively easier. Therefore, it is considered to be necessary to assist authorized use of copyrighted material or to eliminate unauthorized use thereof from the viewpoint of information technology, and to expand the protection of copyrights.

[0005] In the digital content world, as one means for stopping illegal copying, a technique called "digital watermarking" or "data hiding" can be cited. The "digital watermarking" means that information is embedded into content such as images, music, etc., in a barely visible or barely audible form. For example, as a result of embedding copyright information by digital watermarking, the watermark, that is, the copyright information, can be isolated when the content is extracted at a later time, so that the data distribution channel and the presence or absence of a use right can be ascertained.

[0006] For example, in the music record industry and in the broadcast industry, attempts are considered in which use of authored material is automatically managed by embedding an ISRC (International Standard Recording Code), which is identification information provided uniquely for each musical piece, as copyright information, into music content.

[0007] Between music record companies as copyright owners and broadcasting stations as copyright users, for example, a contract is signed such that the copyright royalty is paid in an amount corresponding to the number of times each musical piece is broadcast. Therefore, it is possible for the music record company (or a monitoring company entrusted by a record company) to count the number of times each musical piece is used on the basis of the appearance of the ISRC by receiving the broadcast wave and decrypting the embedded digital watermark. Furthermore, even if the broadcasting station does not accurately or honestly declare the copyright royalty, it would be possible for the music record company to reveal an erroneous declaration on the basis of the count value and to impose a penalty, such as canceling a copyright-use contract, as necessary.

[0008] In order to thoroughly stop copyright infringement by utilizing the ISRC, it is desired that an ISRC be embedded in each musical piece at the time the music content is stored (that is, manufactured) on a storage medium, such as a CD (Compact Disc) .

[0009] However, dependence on the above-described method would make it impossible to track or monitor use of music content played back from a conventional CD before digital watermarks were embedded. Furthermore, it is almost impossible to replace all existing content with new content having digital watermarks.

[0010] In addition, in order to add digital watermarks into all content, a data field of 60 bits is required only for music, causing the overall record length to be increased considerably.

[0011] Various respective aspects and features of the invention are defined in the appended claims.

[0012] Embodiments of the present invention relate to content distribution techniques for distributing or providing content among remote locations, and in particular, relate to content a distribution technique for distributing or providing content to a large number of people, for example, in the form of broadcast waves and network transfer. More particularly, embodiments of the present invention relate to content distribution techniques for a content creator, etc., to securely distribute or provide content having predetermined use rights, including copyrights, such as for music, video, etc., and in particular, relates to a content distribution technique for owners of content rights to distribute or provide contents or to appropriately manage or monitor distribution status.

[0013] The present invention has been achieved in view of the above-described details. Embodiments of the present invention can provide a superior content distribution technique which is capable of distributing or providing content to a large number of people, for example, in the form of broadcast waves and network transfer.

[0014] Embodiments of the present invention can provide a superior content distribution technique which is capable of securely distributing or providing content having a predetermined use right, including copyright, such as music, video, etc.

[0015] Embodiments of the present invention can provide a superior content distribution technique in which it is possible for a right owner of content to appropriately manage or monitor a distribution or provision status of the content, and to accurately impose a content royalty.

[0016] Embodiments of the present invention can provide a superior content distribution technique which is capable of appropriately managing or monitoring a distribution or provision status of content with respect to content played back from a recording medium which has already been distributed.

[0017] According to a first aspect of the present invention, there is provided a content distribution system for distributing content owned by a predetermined right owner, comprising: a monitoring apparatus for monitoring the distribution of contents by issuing authentication information showing a content-use consent; and a distribution apparatus for distributing the content with the attached authentication information received from the monitoring apparatus via a predetermined distribution path.

[0018] The monitoring apparatus referred to herein is an apparatus which is operated, for example, by a copyright owner having a copyright on contents, or by a person who is entrusted by the copyright owner with the business of monitoring use of content. In contrast, a distribution apparatus is an apparatus which is operated by a dealer who is entrusted with a content-use consent by the copyright owner. It is preferable that the monitoring apparatus and the distribution apparatus be interconnected by a secure transmission medium, such as a dedicated line, so that authentication information and other various types of information (to be described later) may be exchanged securely.

[0019] In an embodiment to be described later, a description is given by using as an example a case in which content is distributed by a broadcasting station as a content distribution dealer using broadcast waves. However, it should be understood that the distribution referred to in the present invention is not limited to "broadcasts", and can be similarly used for a case in which, for example, a network broadcast service via a LAN (Local Area Network) and the Internet, and content distribution via various types of storage media, such as a CD (Compact Disc), MO (Magnetooptical Disc), or DVD (Digital Versatile Disc), are performed.

[0020] It is possible for the monitoring apparatus to obtain content being distributed in the predetermined distribution path and to determine the validity of a content distribution operation by the distribution apparatus on the basis of whether or not authentication information is attached to the content.

[0021] The authentication information which is issued by the monitoring apparatus may be formed of the set of time identification information showing the current time and distributor identification information assigned to the distribution apparatus.

[0022] The monitoring apparatus may issue an encryption key in addition to the authentication information. In such a case, the distribution apparatus can distribute content with attached authentication information encrypted using the encryption key received from the monitoring apparatus via a predetermined distribution path. Therefore, it is possible to appropriately prevent the authentication information attached to the content from being falsified in the distribution path.

[0023] The distribution apparatus may embed authentication information into content by using a digital watermarking technique. Alternatively, the distribution apparatus may embed authentication information into a content distribution signal by using a digital watermarking technique. As a result of using a digital watermarking technique, ordinary viewers and listeners who receive a broadcast wave need not be aware of the presence of the authentication information. In particular, in the latter case, since the authentication information need not be embedded into the content itself, authentication information can be easily embedded into music content as well played back from a storage medium which has already been distributed.

[0024] Normally, each content has a specific content identifier. For example, in the case of a music content, an ISRC (International Standard Recording Code), which can be identified anywhere in the world, is assigned to each musical piece.

[0025] It is possible for the distribution apparatus to store the distribution history of each content distributed via the predetermined distribution path in such a manner as to be associated with content identification information.

[0026] In the monitoring apparatus, identification information by which the distribution history can be addressed may be contained in the authentication information. In this case, time identification information need not be contained in the authentication information.

[0027] Furthermore, it is possible for the distribution apparatus to extract only the history information associated with specific content by masking the distribution history with a predetermined filter and to transfer it to a monitoring dealer such as a monitoring apparatus. In the case of the above-described ISRC, it is formed of five groups 1 to 5. Of these, three digits corresponding to group 3 indicate a first owner code. By performing filtering by using this group 3 as a mask, it is possible to extract only the distribution history information relating to the contents of a specific copyright owner. In contrast, on the monitoring apparatus side, the distribution status of each content can be managed on the basis of the distribution history information. For example, it is possible to charge an accurate copyright royalty, corresponding to the number of times the content is used, to the distribution apparatus, that is, the broadcasting station.

[0028] According to a second aspect of the present invention, there is provided a content distribution method for distributing content owned by a predetermined right owner, comprising: a first step of issuing authentication information showing a content-use consent; a second step of distributing the content with the attached authentication information issued in the first step via a predetermined distribution path; and a third step of monitoring the distribution of the content in the distribution path.

[0029] The above-described third step can obtain content being distributed in the predetermined distribution path and determine the validity of the content distribution operation on the basis of whether or not the authentication information is attached to the content.

[0030] The above-described first step may issue, as the authentication information, the set of time identification information showing the current time and distributor identification information assigned to the distribution of the content.

[0031] Furthermore, the above-described first step may issue an encryption key in addition to the authentication information. In this case, the above-described second step can distribute the content via the predetermined distribution path with attached authentication information encrypted using the encryption key issued in the first step, making it possible to appropriately prevent the authentication information from being falsified.

[0032] The above-described second step may embed the authentication information into the content by using a digital watermarking technique. Alternatively, the second step may embed the authentication information into a distribution signal of the content by using a digital watermarking technique.

[0033] Each content usually has specific content identification information. In such a case, it is possible to further provide a fourth step of storing the distribution history of each content distributed via the predetermined distribution path in the second step in such a manner as to be associated with the content identification information. Furthermore, identification information by which the distribution history can be addressed may be contained in the authentication information. In this case, time identification information need not be contained in the authentication information. It is possible to further provide a fifth step of extracting only the history information associated with specific content by masking the distribution history with a predetermined filter and a sixth step of managing a state in which each content is distributed on the basis of the distribution history.

[0034] According to a third aspect of the present invention, there is provided a content monitoring apparatus or method for monitoring the use of a content owned by a predetermined right owner, wherein means is provided for issuing authentication information showing a use consent to a content user.

[0035] The authentication information may contain at least time identification information showing the current time and distributor identification information assigned to the distributor.

[0036] An encryption key may be issued in addition to the authentication information.

[0037] A means or a step for obtaining the contents being used and checking the presence or absence of authentication information may be further provided.

[0038] A means or a step for managing a content use status on the basis of the content use history of a content user may be further provided.

[0039] According to a fourth aspect of the present invention, there is provided a content using apparatus or method for using contents after receiving a consent from a predetermined right owner, comprising: receiving means or step for receiving authentication information showing a content-use consent from the outside; and using means or step for using the contents with the received authentication information attached.

[0040] The using means or step can distribute the contents with the authentication information via a predetermined distribution path. As a result, the validity of the content can be checked on the basis of whether or not authentication information is contained in the content to be used in the distribution path.

[0041] The authentication information can contain at least time identification information showing the current time and user identification information assigned to the user.

[0042] The receiving means or step may receive an encryption key in addition to the authentication information, and the using means or step may use the contents with attached authentication information encrypted using the encryption key. As a result, it is possible to appropriately prevent the authentication information from being falsified in the distribution path.

[0043] The using means may embed authentication information into content by using a digital watermarking technique. Alternatively, the using means or step may embed authentication information into a content distribution signal by using a digital watermarking technique.

[0044] Each content usually has specific content identification information. Therefore, history information storage means or step can store the use history of each content used in the using means or step in such a manner as to be associated with the content identification information. Furthermore, identification information by which the use history can be addressed may be contained in the authentication information. In this case, time identification information need not be contained in the authentication information.

[0045] It is possible to extract only history information associated with a specific content by masking the stored use history with a specific filter. It is also possible to manage the use status of each content on the basis of the stored use history.

[0046] The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

Fig. 1 is a diagram schematically showing the configuration of a content distribution system 100 according to an embodiment of the present invention;
Fig. 2 is a diagram schematically showing another configuration of the content distribution system 100 according to the embodiment of the present invention;
Fig. 3A is a schematic representation of a state in which authentication information which is embedded by digital watermark is encrypted, showing a state in which authentication information composed of a time ID and a broadcasting station ID is encrypted;
Fig. 3B is a schematic representation of a state in which authentication information which is embedded by digital watermark is encrypted, showing a state in which a time ID in the form of plain text is attached to the encrypted authentication information; and
Fig. 4 is a diagram showing in detail the configuration of the content distribution system 100 according to the embodiment of the present invention.

[0047] An embodiment of the present invention will be described below with reference to the attached drawings.

[0048] Fig. 1 schematically shows the concept of a content distribution system 100 according to the present invention. As shown in Fig. 1, the content distribution system 100 comprises a broadcasting station 10 and a monitoring station 50.

[0049] The monitoring station 50 is operated by the copyright owner or is operated by an organization or company which is entrusted by the copyright owner so as to track or monitor the use of authored material. The copyright owner may be a music record company which stores music contents in recording media, such as CDs, and which sells and distributes them. Also, the monitoring station 50 monitors each content, that is, each piece of authored material, which is used in broadcasting by the broadcasting station, and the detailed procedure thereof will be described later.

[0050] In the example shown in Fig. 1, a monitoring station is set for each copyright owner. However, as shown in Fig. 2, a single monitoring station may provide monitoring services for use of content to plural copyright owners.

[0051] Also, in actuality, there is a plurality of broadcasting stations, and the copyright owner must monitor the copyright owner's own authored material, that is, the content use status, for all the broadcasting stations. The copyright owner may set up a monitoring station for each broadcasting station, or a single monitoring station may handle plural broadcasting stations.

[0052] In the following, for the sake of convenience, a description is given by using, as an example, a case in which one monitoring station 50 monitors one broadcasting station 10.

[0053] The broadcasting station 10 and the monitoring station 50 are interconnected with each other via a secure transmission line, such as a dedicated line 20, and what is commonly called "impersonation" can be blocked by causing a predetermined authentication procedure to be performed.

[0054] During the period in which authentication is being established between them, the monitoring station 50 supplies, to the broadcasting station 10, broadcasting station identification information (hereinafter referred to as a "broadcasting station ID"), time identification information (hereinafter referred to as a "time ID"), and an encryption key. In the following, the information composed of the combination of the broadcasting station ID and the time ID is called "authentication information". The authentication information enables authentication of a use consent for content.

[0055] However, the time identification information need not necessarily be contained in the authentication information. For example, the time identification information may be replaced with another identification information by which each record of the broadcast information (to be described later) stored in the broadcast station can be addressed.

[Broadcasting station ID] : [Time ID] : [Key]

[0056] The broadcasting station ID is a proof such that the monitoring station 50 which handles content use for the copyright owner has authenticated the broadcasting station 10, and further, has consented to the use of the authored material. When the monitoring station 50 consents to the use of authored material in a constant or fixed manner, the monitoring station 50 need only transfer the broadcasting station ID to the broadcasting station 10 only once after authentication has been established. When, on the other hand, use of authored material is consented to only in a time-limited manner, it is necessary to transfer a new broadcasting station ID to the broadcasting station 10 each time use of the authored material is newly consented to during the period in which the authentication has been established. The time-limited broadcasting station ID can be managed in combination with, for example, the time ID (to be described later). In the case of the implementation of the latter case, the monitoring station 50 can supply a consent for using the authored material for each broadcast program or for each broadcast time zone.

[0057] Furthermore, the time ID is identification information which is uniquely related to the current time, and, for example, may be the time data itself. When the provision of the time ID by the monitoring station 50 and the content distribution in the broadcasting station 10, that is, a program broadcast, are being performed in real time (or when the time lag between the provision of the time ID and the content distribution is a fixed value), the time ID can specify the broadcast time of a program and the broadcast content itself.

[0058] The key is an encryption key which is used to encrypt predetermined authentication information composed of the broadcasting station ID and the time ID on the broadcasting station 10 side and to further decrypt the encrypted information in the monitoring station 50. When one key is used in a fixed manner, the monitoring station 50 need only transfer the key only once to the broadcasting station 10 after the authentication has been established. However, in order to prevent reuse of a key, it is necessary for the monitoring station 50 to change the key as time elapses and to transfer the key to the broadcasting station 10 each time the key is changed. In the case of the latter case, the key can be recognized as a time-related function key (t). The key (t) may be managed in association with the time ID.

[0059] For the key used herein, either a common key encryption method in which the same key is used at the time of encryption and decryption or a public key encryption method in which a secret key and a public key are formed in combination may be used. However, in the following description, for the sake of convenience, a common key is used.

[0060] On the broadcasting station 10 side, a broadcast wave in which the authentication information received from the monitoring station 50 is superposed onto the distribution content is generated, and the broadcast wave is transmitted that is, broadcast, to each receiver.

[0061] The authentication information, as described above, is composed of the combination (for example, each ID is bit-coupled) of the broadcasting station ID and the time ID. When a broadcast is performed in real time with the authentication by the broadcasting station 10, the time ID may be omitted. However, on the receiver side, in order to specify the source of the broadcast content stored on a recording medium, that is, the copyright owner of the authored material, it is preferable that the time ID be used as a part of the authentication information.

[0062] In realizing the present invention, the form in which the authentication information is attached to the broadcast content does not particularly matter. For example, the broadcasting station ID and the time ID may be superposed on each other by using a digital watermarking technique. In such a case, the authentication information may be superposed on either the content itself or on the broadcast wave. As a result of using a digital watermarking technique, it is not at all necessary for receivers such as ordinary viewers and listeners to be concerned with the presence of the authentication information.

[0063] When digital watermarking is performed on a broadcast wave rather than on the original content, the present invention can be applied by merely changing the equipment of the broadcasting station. Also, since the digital watermark need not be provided in the content itself, it is possible to appropriately perform copyright management on a content which originates from a recording medium such as a CD, which has already been in common use.

[0064] Furthermore, in order that the authentication information which is embedded by digital watermarking be protected against falsification, the authentication information composed of the broadcasting station ID and the time ID may be encrypted (see Fig. 3A) using the key received from the monitoring station 50, after which the authentication information is superposed onto the broadcast wave. In such a case, it is necessary for the monitoring station 50 to decrypt the authentication information. Furthermore, when the key is a function of time, key (t), the monitoring station 50 must determine which key should be used for decryption. Therefore, the information (see Fig. 3B) in which a time ID in the form of plain text is further attached to the encrypted authentication information may be superposed onto the broadcast wave. It is possible for the monitoring station 50 to determine the applicable key (t) on the basis of the time ID.

[0065] The broadcasting station 10 stores the broadcast history information about the contents which are broadcast by the broadcasting station 10 itself so as to manage a database. For the database, it is preferable that records be created for each broadcast content. Each record has fields for storing each of at least a content ID, a time ID, and a broadcasting station ID, as shown below:

[Content ID] : [Time ID] : [Broadcasting station ID]

[0066] The content ID referred to herein is information by which a broadcast content can be uniquely identified. For example, in the case of a music content, an ISRC which is defined in the ISO (International Organization for Standardization) 3901 can be used. Furthermore, in the case of a commercial, an ISCI can be used. In addition to these, a tag affixed to a sequence may be used content ID.

[0067] The history information which is formed into a database is transferred to the monitoring station 50 as necessary (for example, in response to a request). Alternatively, the monitoring station 50 can access the history information database independently.

[0068] Fig. 4 shows in more detail the configuration of the content distribution system 100 according to the embodiment of the present invention.

[0069] As shown in Fig. 4, the monitoring station 50 comprises a monitor server 51, a clock 52 for providing the current time, and one or more receivers 53A and 53B for receiving the broadcast wave of the broadcasting station 10. It is assumed that the monitor server 51 is connected to each section by a secure communication method, such as encrypted communication.

[0070] The monitor server 51 is connected to the management server 11 through a secure transmission line, such as the dedicated line 20, so that authentication can be established between the monitoring station 50 and the broadcasting station 10 in accordance with a predetermined procedure. As a result of establishing the authentication, the monitor server 51 can supply authentication information, such as the broadcasting station ID and the time ID, and the key to the broadcasting station 10.

[0071] The broadcasting station 10 comprises a management server 11 for centrally managing the operations within the station, a playback unit 12, an editing unit 13, a broadcast server 14, a digital-watermark embedding section 15, a transmitter 16, and a broadcast history database 17. It is assumed that the management server 11 is connected to each section by a secure communication method, such as encrypted communication.

[0072] The playback unit 12 plays back content in media, such as music, video, announcements, etc. Also, the editing unit 13 integrates and edits each played-back content in media in order to edit a broadcast content. The edited results are stored in the broadcast server 14.

[0073] The broadcast server 14 is connected to the management server 11 at all times by a secure communication method, such as encrypted communication. Thus, the broadcast history about media playback, and the broadcast content editing and recording can be securely stored in the broadcast history database 17. In the broadcast history database 17, for example, records are created for each broadcast content, and each record has fields for storing each of at least a content ID, a time ID, and a broadcasting station ID, as described earlier.

[0074] Also, the broadcast server 14 completes the editing results by the editing unit 13 in form in which they can be distributed as broadcast waves, and outputs these at a scheduled time (for example, a broadcast time) controlled by the management server 11.

[0075] The digital-watermark embedding section 15 embeds the authentication information received from the monitor server 51 as a digital watermark. The authentication information is composed of-the broadcasting station ID and the time ID. In this case, in order that the falsification of the authentication information be prevented, it is preferable that the authentication information be embedded after being encrypted using the key received from the monitor server 51. Furthermore, in order to improve the level of security, it is preferable that the key be changed as time elapses. In this case, in order to make it easy to determine the key used, the encrypted authentication information to which a time ID in the form of plain text is attached may be embedded (see description above and Fig. 3B).

[0076] The transmitter 16 emits a broadcast wave in which authentication information is embedded in a manner as described above. The broadcast wave, however, may be a terrestrial wave or a satellite wave, and the transmission line may be either wireless or cables. Furthermore, as a modification of the present invention, the path of the content distribution may be for content distribution through a network such as a LAN (Local Area Network) or the Internet, or through a public telephone network such as PSTN (Public Switched Telephone Network) or ISDN (Integrated Services Digital Network). Furthermore, the content distribution form may be either a push type or a pull type.

[0077] The management server 11 and the monitor server 51 are connected to each other through a secure transmission line such as a dedicated line, so that authentication can be established between the monitoring station 50 and the broadcasting station 10 in accordance with a predetermined procedure. As a result of establishing the authentication, the management server 11 can supply, to the monitor server 51, history information stored in the broadcast history database 17 as necessary (for example, in response to a request). Alternatively, the monitor server 51 can access the history information database.

[0078] The broadcasting station 10 usually produces a broadcast program by using the contents of a plurality of copyright owners. Also, as shown in Fig. 1, there are cases in which one broadcasting station 10 is placed under the supervision of a plurality of monitoring stations 50 which are set for each copyright owner. In such a case, transmitting all the records stored in the broadcast history database 17 to all the monitor stations 50A, 50B, ..., is inefficient and irrational. The reason for this is that disclosure of the use status of the authored material to those other than the copyright owner corresponds to an invasion of privacy, and transferring of more data than is necessary increases the communication load unnecessarily. Therefore, the history information should be filtered for each copyright owner and transmitted to the monitoring station 50.

[0079] For example, in the case of the ISRC assigned to the music content, it is formed of five groups 1 to 5. Of these, three digits corresponding to group 3 indicate a first owner code. By performing filtering by using this group 3 as a mask, it is possible to extract only the history information relating to the contents of a specific copyright owner. In contrast, on the monitoring station 50 side, the distribution status of each content can be managed on the basis of the history information. For example, it is possible to charge an accurate copyright royalty, corresponding to the number of times the content is used, to the distribution apparatus, that is, the broadcasting station.

[0080] Next, a description is given of the processing procedure for monitoring the use status of a piece of authored material in the monitoring station 50. However, the authored material referred to herein refers to a music content used during a broadcast program in the broadcasting station 10, the user of the authored material is the broadcasting station 10, and the monitoring object is a broadcast wave emitted from the broadcasting station 10.

[0081] When the monitoring receivers 53A and 53B receive a broadcast wave, the monitoring receivers 53A and 53B decode the digital watermark in order to extract the authentication information, and transfers this to the management server 11 in a secure form.

[0082] It is possible for the management server 11 to confirm that the broadcasting station 10 is using the authored material, that is, a content, with authorization based on the fact that the authentication information is contained in the broadcast wave. When the authentication information is not contained in the content, since this means that the broadcasting station 10 is using the authored material without authorization, a penalty may be imposed on the broadcasting station 10. The penalty may be an action for depriving or suspending the content use right for a predetermined period.

[0083] Furthermore, embedding the authentication information encrypted using a key by the broadcasting station 10 makes it possible to determine whether or not there has been impersonation in the distribution path. That is, when the authentication information cannot be decoded using a key corresponding to the broadcast content, it can be determined that impersonation has occurred. Also, when authentication information in a form such as that shown in Fig. 3B is embedded, a case in which the time ID attached in plain text does not match the time ID obtained by decoding the authentication information can be determined as being a case of impersonation.

[0084] The management server 11 monitors the system from the playback unit 12 up to the transmitter 16, and confirms that the content is not falsified, after which the management server 11 requests the monitor server 51 to issue a key. As a result, only the broadcast history information whose security has been confirmed is stored in the broadcast history database 17.

[0085] The present invention has thus been described in detail while referring to a specific embodiment. It is self-explanatory that modifications and substitutions of the embodiment may be made without departing from the spirit and scope of the present invention by a person skilled in the art.

[0086] In the above-described embodiment, an ISRC, tags affixed to a sequence, etc., are used, as a content ID, for the digital watermark, but the content ID is not particularly limited thereto. For example, even if data in which a part or all of a musical piece is compressed or data in which a part of a musical piece is sampled, is used for the digital watermark, the same operational effects can be obtained.

[0087] In summary, the present invention has been disclosed in the form of exemplifications and should not be construed as being limited thereby. In order to determine the gist of the present invention, the claims should be taken into consideration.

[0088] As has thus been described in detail, according to the present invention, it is possible to provide a superior content distribution technique which is capable of distributing or providing content to a large number of people, for example, in the form of broadcast waves and network transfer.

[0089] According to embodiments of the present invention, it is possible to provide a superior content distribution technique which is capable of securely distributing or providing content having a predetermined use right, including copyright, such as music, video, etc.

[0090] According to embodiments of the present invention, it is possible to provide a superior content distribution technique in which it is possible for a right owner of content to appropriately manage or monitor a distribution or provision status of the content.

[0091] According to embodiments of the present invention, it is possible to provide a superior content distribution technique which is capable of appropriately managing or monitoring a distribution or provision status of content with respect to content played back from a recording medium which has already been distributed.

[0092] According to embodiments of the present invention, as a result of performing digital watermarking on a broadcast wave rather than on the original content, adaptations are possible by merely changing the equipment of the broadcasting station. Furthermore, since the digital watermark need not be provided in the content itself, it is possible to appropriately perform copyright management on a content which originates from a recording medium such as a CD, which has already been in common use.

[0093] Many different embodiments of the present invention may be constructed without departing from the scope of the present invention. It should be understood that the present invention is not limited to the specific embodiment described in this specification. To the contrary, the present invention is intended to cover various modifications and equivalent arrangements included within the scope of the invention as hereafter claimed. The scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications, equivalent structures and functions.

Claims

1. A content distribution system for distributing content owned by a predetermined right owner, comprising:

   a monitoring apparatus for monitoring the distribution of contents by issuing authentication information showing a content-use consent; and

   a distribution apparatus for distributing the content with the attached authentication information received from said monitoring apparatus via a predetermined distribution path.

2. A content distribution system according to claim 1, wherein said monitoring apparatus obtains the content being distributed in said predetermined distribution path and determines the validity of the content distribution operation by the distribution apparatus on the basis of whether or not the authentica-

tion information is attached to the content.

3. A content distribution system according to claim 1, wherein said monitoring apparatus issues, as authentication information, the set of time identification information showing the current time and distributor identification information assigned to the distribution apparatus.

4. A content distribution system according to claim 1, wherein said monitoring apparatus issues an encryption key in addition to the authentication information, and said distribution apparatus distributes the content with the attached authentication information encrypted using the encryption key received from said monitoring apparatus.

5. A content distribution system according to claim 1, wherein said distribution apparatus embeds the authentication information into the content by using a digital watermarking technique.

6. A content distribution system according to claim 1, wherein said distribution apparatus embeds the authentication information into a distribution signal of the content by using a digital watermarking technique.

7. A content distribution system according to claim 1, wherein each content has specific content identification information, and said distribution apparatus stores the distribution history of each content distributed via said predetermined distribution path in such a manner as to be associated with the content identification information.

8. A content distribution system according to claim 1, wherein each content has specific content identification information, said distribution apparatus stores the distribution history of each content distributed via said predetermined distribution path in such a manner as to be associated with the content identification information, and transfers only the history information associated with specific content by masking the distribution history with a predetermined filter.

9. A content distribution system according to claim 1, wherein each content has specific content identification information, said distribution apparatus stores the distribution history of each content distributed via said predetermined distribution path in such a manner as to be associated with the content identification information, and said monitoring apparatus manages the distribution status of each content on the basis of the distribution history.

10. A content distribution system according to claim 1, wherein each content has specific content identification information, said distribution apparatus stores the distribution history of each content distributed via said predetermined distribution path in such a manner as to be associated with the content identification information, and said monitoring apparatus causes identification information by which the distribution history can be addressed to be contained in said authentication information.

11. A content distribution method for distributing content owned by a predetermined right owner, comprising:

a first step of issuing authentication information showing a content-use consent;
a second step of distributing the content via a predetermined distribution path with the attached authentication information issued in said first step; and
a third step of monitoring the distribution of the content in said distribution path.

12. A content distribution method according to claim 11, wherein said third step obtains content being distributed in said predetermined distribution path and determines the validity of the content distribution operation on the basis of whether or not authentication information is attached to the content.

13. A content distribution method according to claim 11, wherein said first step issues, as authentication information, the set of time identification information showing the current time and distributor identification information assigned to the distribution of the content.

14. A content distribution method according to claim 11, wherein said first step issues an encryption key in addition to the authentication information, and said second step distributes the content via said predetermined distribution path with the attached authentication information encrypted using the encryption key issued in said first step.

15. A content distribution method according to claim 11, wherein said second step embeds authentication information into the content by using a digital watermarking technique.

16. A content distribution method according to claim 11, wherein said second step embeds authentication information into a distribution signal of the content by using a digital watermarking technique.

17. A content distribution method according to claim 11, each content having specific content identification information, said content distribution method further

comprising:

a fourth step of storing the distribution history of each content distributed via said predetermined distribution path in said second step in such a manner as to be associated with the content identification information.

18. A content distribution method according to claim 11, each content having specific content identification information, said content distribution method further comprising:

a fourth step of storing the distribution history of each content distributed via said predetermined distribution path in said second step in such a manner as to be associated with the content identification information; and
a fifth step of extracting only the history information associated with specific content by masking the distribution history with a predetermined filter.

19. A content distribution method according to claim 11, each content having specific content identification information, said content distribution method further comprising:

a fourth step of storing the distribution history of each content distributed via said predetermined distribution path in said second step in such a manner as to be associated with the content identification information; and
a sixth step of managing a state in which each content is distributed on the basis of the distribution history.

20. A content distribution method according to claim 11, each content having specific content identification information, said content distribution method further comprising:

a fourth step of storing the distribution history of each content distributed via said predetermined distribution path in said second step in such a manner as to be associated with the content identification information,
wherein said first step issues authentication information in such a manner as to contain identification information by which the distribution history can be addressed.

21. A content monitoring apparatus for monitoring the use of content owned by a predetermined right owner, said content monitoring apparatus comprising:

means for issuing authentication information showing a use consent to a content user.

22. A content monitoring apparatus according to claim 21, wherein said authentication information contains at least time identification information showing the current time and distributor identification information assigned to the distributor.

23. A content monitoring apparatus according to claim 21, wherein said authentication information contains at least distributor identification information assigned to the distributor and identification information by which the distribution history of the content in the distributor can be addressed.

24. A content monitoring apparatus according to claim 21, wherein an encryption key is issued in addition to the authentication information.

25. A content monitoring apparatus according to claim 21, further comprising:

means for-obtaining the content being used and checking the presence or absence of the authentication information.

26. A content monitoring apparatus according to claim 21, further comprising:

means for managing a content use status on the basis of the content use history of a content user.

27. A content monitoring method for monitoring use of content owned by a predetermined right owner, comprising the step of:

issuing authentication information showing a use consent to a content user.

28. A content monitoring method according to claim 27, wherein said authentication information contains at least time identification information showing the current time and distributor identification information assigned to the distributor.

29. A content monitoring method according to claim 27, wherein said authentication information contains at least distributor identification information assigned to the distributor and identification information by which the distribution history of the content in the distributor can be addressed.

30. A content monitoring method according to claim 27, wherein an encryption key is issued in addition to the authentication information.

31. A content monitoring method according to claim 27, comprising the step of:

obtaining the content being used and checking the presence or absence of the authentication information.

32. A content monitoring method according to claim 27, comprising the step of:

managing a content use status on the basis of the content use history of a content user.

33. A content using apparatus for using content after receiving a consent from a predetermined right owner, comprising:

receiving means for receiving authentication information showing a content-use consent from the outside; and
using means for using the content with the received authentication information attached.

34. A content using apparatus according to claim 33, wherein said using means distributes the content with the authentication information via a predetermined distribution path.

35. A content using apparatus according to claim 33, wherein said authentication information contains at least time identification information showing the current time and user identification information assigned to the user.

36. A content using apparatus according to claim 33, wherein said authentication information contains at least distributor identification information assigned to the distributor and identification information by which the use history of the content in the distributor can be addressed.

37. A content using apparatus according to claim 33, wherein said receiving means receives an encryption key in addition to the authentication information, and said using means uses the content with attached authentication information encrypted using the encryption key.

38. A content using apparatus according to claim 33, wherein said using means embeds the authentication information into the content by using a digital watermarking technique.

39. A content using apparatus according to claim 33, wherein said using means embeds the authentication information into a distribution signal of the content by using a digital watermarking technique.

40. A content using apparatus according to claim 33, each content having specific content identification information, said content using apparatus further comprising:

history information storage means for storing the use history of each content used in said using means in such a manner as to be associated with the content identification information.

41. A content using apparatus according to claim 33, each content having specific content identification information, said content using apparatus further comprising:

history information storage means for storing the use history of each content used in said using means in such a manner as to be associated with the content identification information; and
history information extraction means for extracting only the history information associated with specific content from said history information storage means by masking the stored use history with a predetermined filter.

42. A content using apparatus according to claim 33, each content having specific content identification information, said content using apparatus further comprising:

history information storage means for storing the use history of each content used in said using means in such a manner as to be associated with the content identification information; and
use status management means for managing a use status of each content on the basis of the stored use history.

43. A content using method for using content after receiving a consent from a predetermined right owner, comprising:

a receiving step of receiving authentication information showing a content-use consent from the outside; and
a using step of using the content with the received authentication information attached.

44. A content using method according to claim 43, wherein said using step distributes the content with the authentication information via a predetermined distribution path.

45. A content using method according to claim 43, wherein said authentication information contains at least time identification information showing the current time and user identification information assigned to the user.

46. A content using method according to claim 43, wherein said authentication information contains at least distributor identification information assigned to the distributor and identification information by which the use history in the distributor can be addressed.

47. A content using method according to claim 43, wherein said receiving step receives an encryption key in addition to the authentication information, and said using step uses the content with the attached authentication information encrypted using the encryption key.

48. A content using method according to claim 43, wherein said using step embeds authentication information into the content by using a digital watermarking technique.

49. A content using method according to claim 43, wherein said using step embeds authentication information into a distribution signal of content by using a digital watermarking technique.

50. A content using method according to claim 43, each content having specific content identification information, said content using method further comprising:

a history information storing step of storing the use history of each content used in said using step in such a manner as to be associated with the content identification information.

51. A content using method according to claim 43, each content having specific content identification information, said content using method further comprising:

a history information storing step of storing the use history of each content used in said using step in such a manner as to be associated with the content identification information; and
a history information extraction step of extracting only the history information associated with specific content by masking the stored use history with a predetermined filter.

52. A content using method according to claim 43, each content having specific content identification information, said content using method further comprising:

a history information storing step of storing the use history of each content used in said using step in such a manner as to be associated with the content identification information; and
a use status managing step of managing a use status of each content on the basis of the stored use history.

FIG. 1

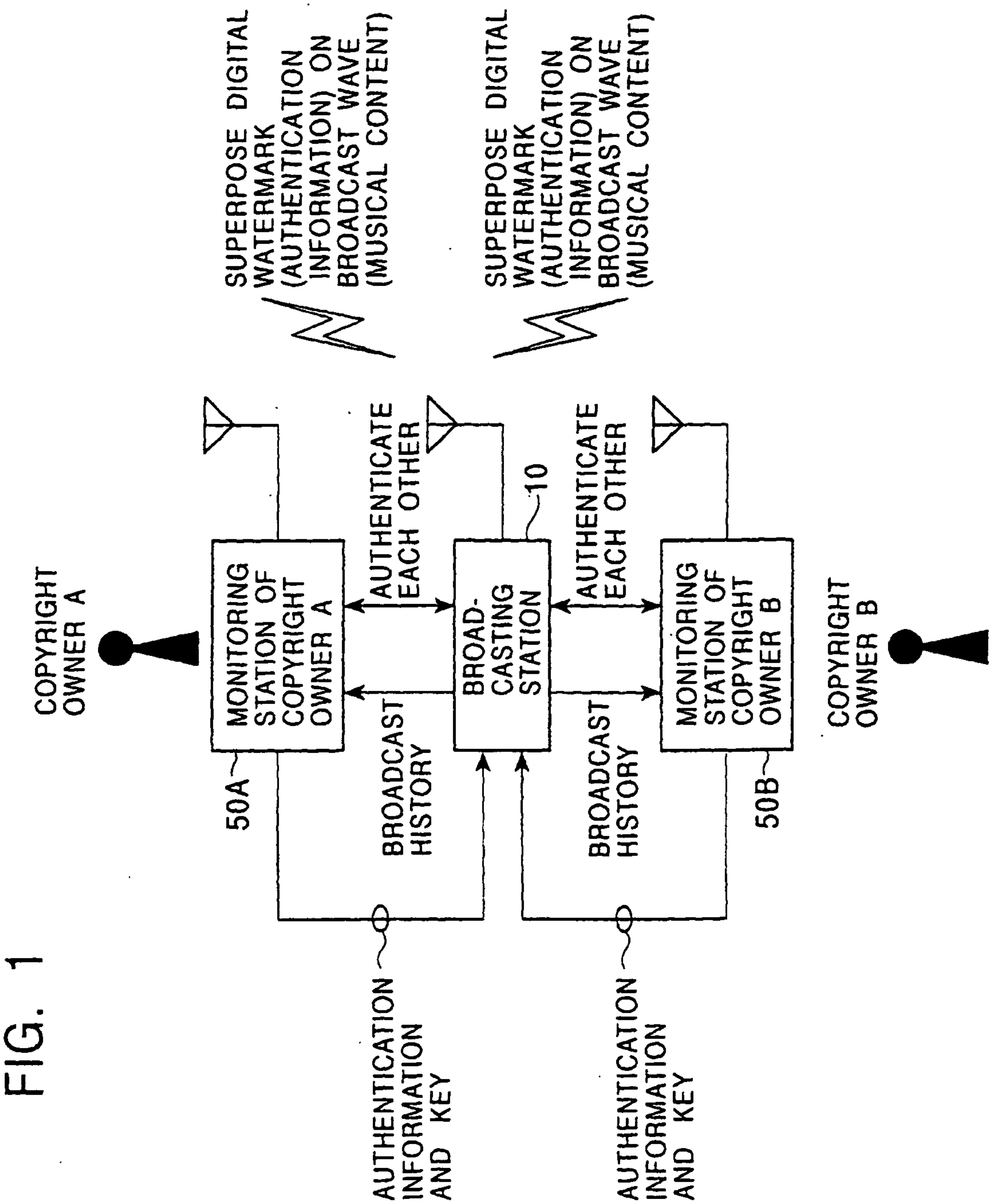

COPYRIGHT OWNER A
MONITORING STATION OF COPYRIGHT OWNER A
50A
AUTHENTICATE EACH OTHER
BROADCAST HISTORY
BROAD-CASTING STATION
10
AUTHENTICATE EACH OTHER
BROADCAST HISTORY
MONITORING STATION OF COPYRIGHT OWNER B
50B
COPYRIGHT OWNER B
AUTHENTICATION INFORMATION AND KEY
AUTHENTICATION INFORMATION AND KEY
SUPERPOSE DIGITAL WATERMARK (AUTHENTICATION INFORMATION) ON BROADCAST WAVE (MUSICAL CONTENT)
SUPERPOSE DIGITAL WATERMARK (AUTHENTICATION INFORMATION) ON BROADCAST WAVE (MUSICAL CONTENT)

FIG. 2

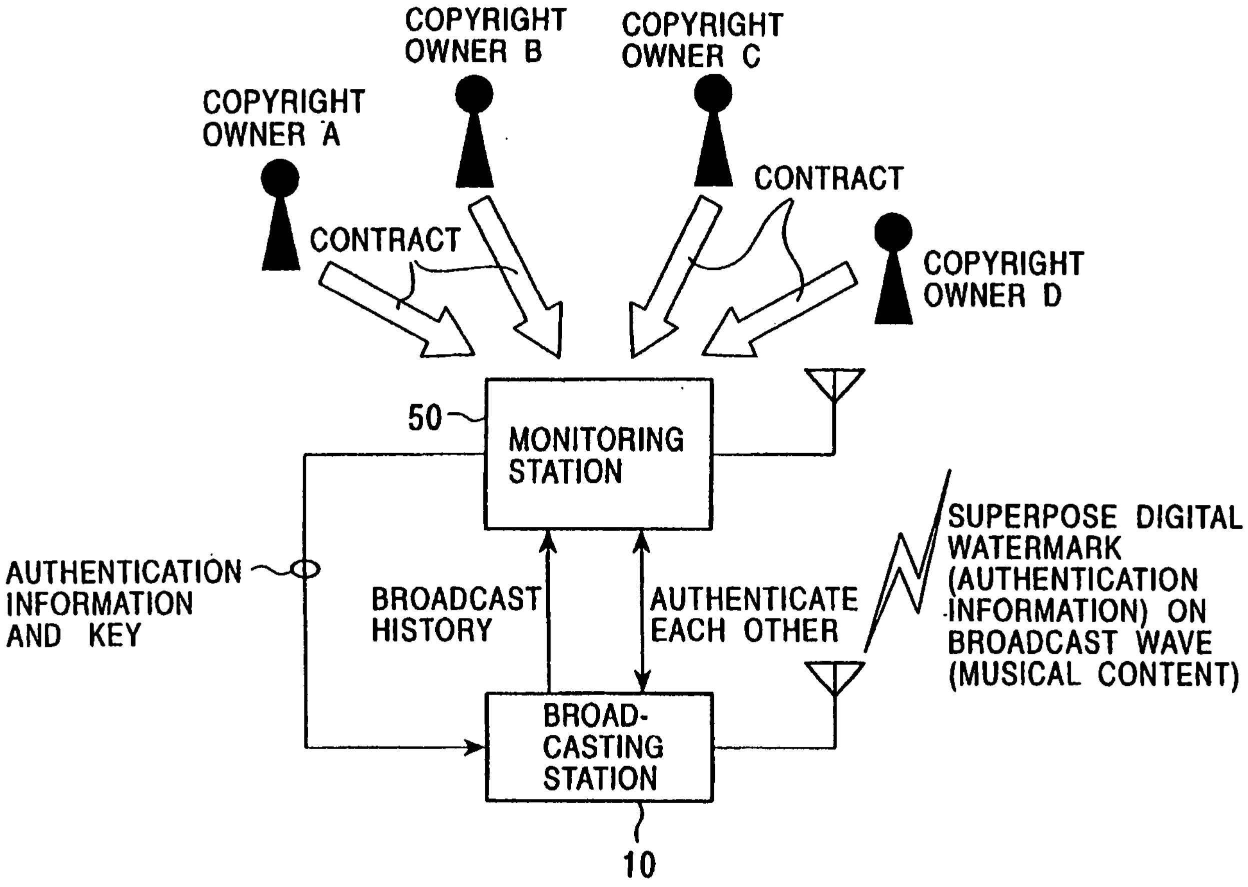

COPYRIGHT OWNER A
COPYRIGHT OWNER B
COPYRIGHT OWNER C
COPYRIGHT OWNER D
CONTRACT
CONTRACT
50
MONITORING STATION
AUTHENTICATION INFORMATION AND KEY
BROADCAST HISTORY
AUTHENTICATE EACH OTHER
SUPERPOSE DIGITAL WATERMARK (AUTHENTICATION INFORMATION) ON BROADCAST WAVE (MUSICAL CONTENT)
BROAD-CASTING STATION
10

FIG. 3A

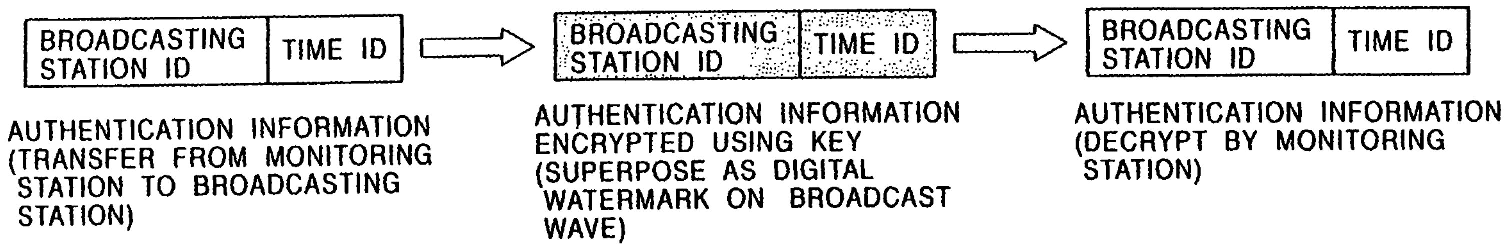

BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION (TRANSFER FROM MONITORING STATION TO BROADCASTING STATION)
BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION ENCRYPTED USING KEY (SUPERPOSE AS DIGITAL WATERMARK ON BROADCAST WAVE)
BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION (DECRYPT BY MONITORING STATION)

FIG. 3B

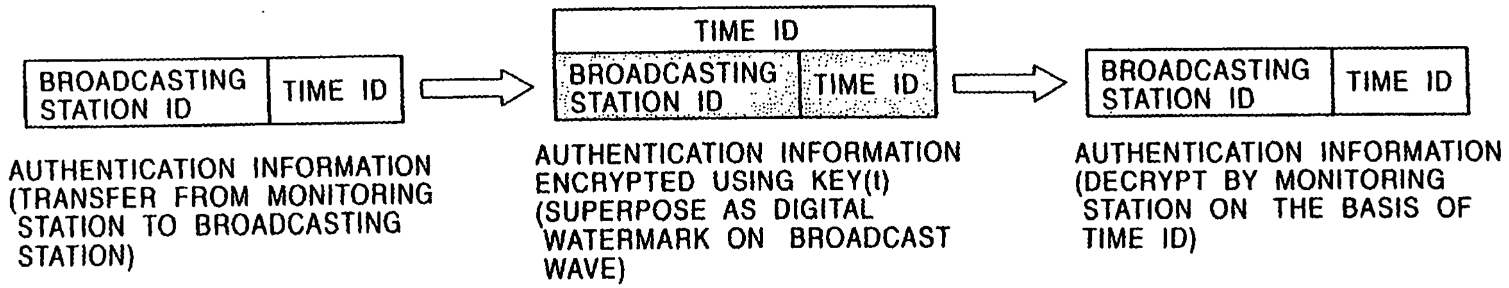
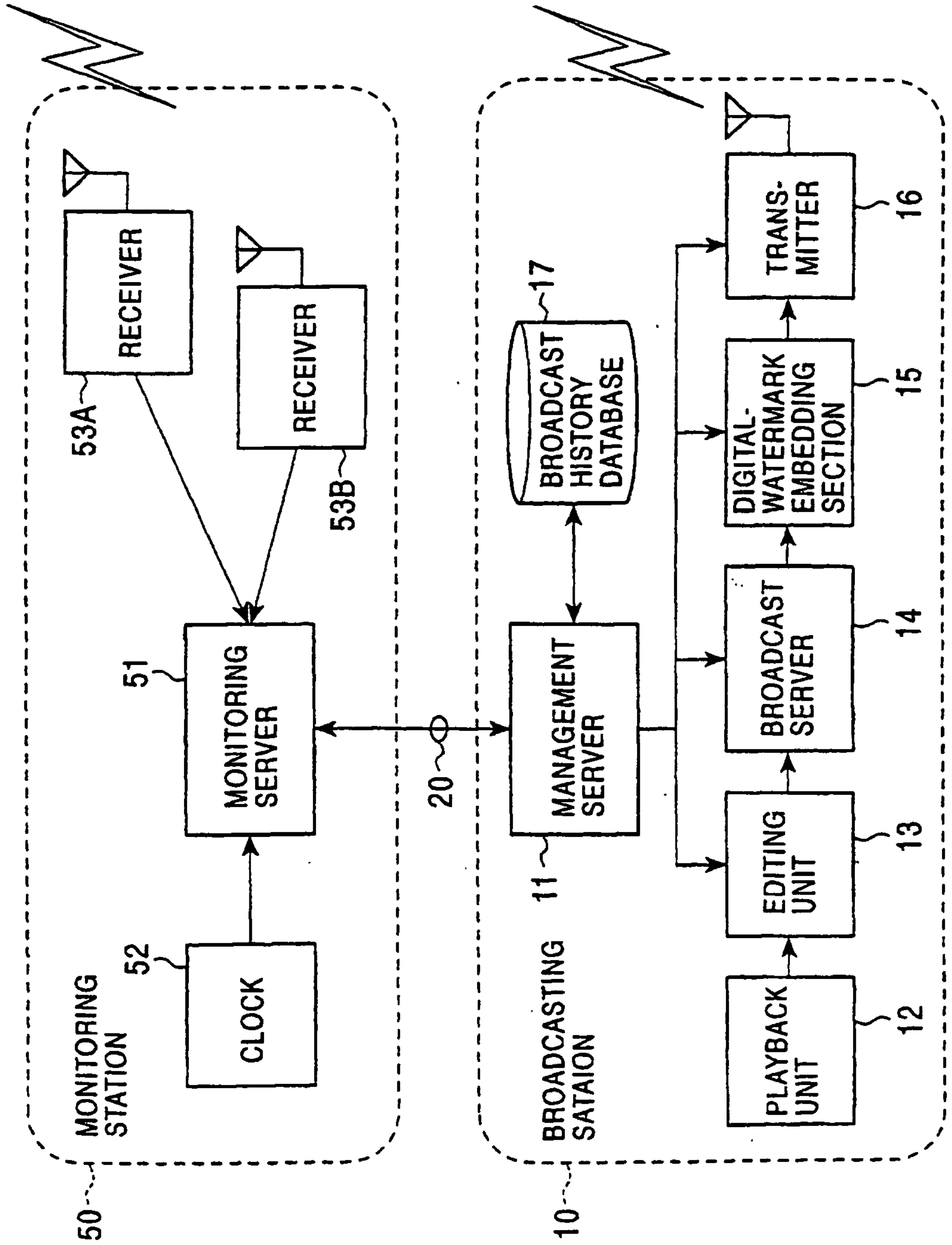

BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION (TRANSFER FROM MONITORING STATION TO BROADCASTING STATION)
TIME ID
BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION ENCRYPTED USING KEY(t) (SUPERPOSE AS DIGITAL WATERMARK ON BROADCAST WAVE)
BROADCASTING STATION ID
TIME ID
AUTHENTICATION INFORMATION (DECRYPT BY MONITORING STATION ON THE BASIS OF TIME ID)

FIG. 4


MONITORING STATION
CLOCK
52
MONITORING SERVER
51
RECEIVER
53A
RECEIVER
53B
50
20
BROADCASTING SATAION
PLAYBACK UNIT
12
EDITING UNIT
13
MANAGEMENT SERVER
11
BROADCAST SERVER
14
BROADCAST HISTORY DATABASE
17
DIGITAL-WATERMARK EMBEDDING SECTION
15
TRANS-MITTER
16
10

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 130 500 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
28.07.2004 Bulletin 2004/31

(43) Date of publication A2:
05.09.2001 Bulletin 2001/36

(21) Application number: **01300144.1**

(22) Date of filing: **09.01.2001**

(51) Int Cl.^{7}: **G06F 1/00**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **20.01.2000 JP 2000014195**

(71) Applicant: **SONY CORPORATION**
Tokyo 141 (JP)

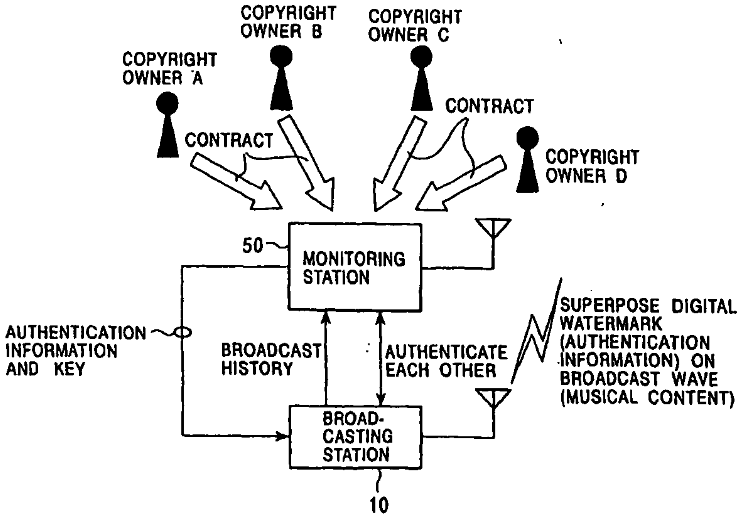
(72) Inventor: **Hirai, Jun,**
Intellectual Property Department
Tokyo 141 (JP)

(74) Representative: **Turner, James Arthur et al**
D. Young & Co.,
21 New Fetter Lane
London EC4A 1DA (GB)

(54) System and method for distribution and monitoring of copyrighted data

(57) In order to appropriately manage or monitor a content distribution status and to accurately impose a content royalty, a content distribution system includes a monitoring apparatus for issuing authentication information showing a content-use consent and monitoring the distribution of a content, and a distribution apparatus for distributing the content via a predetermined distribution path with the attached authentication information. The monitoring apparatus, in which the authentication information is composed of the set of time identification information showing the current time and distributor identification information assigned to the distribution apparatus, obtains a content being distributed in the distribution path, and can determine the validity of the distributed content on the basis of whether or not the authentication information is attached to the content.

FIG. 2



Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 0144

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 893 067 A (MORIMOTO NORISHIGE ET AL) 6 April 1999 (1999-04-06) * column 1, line 5 - line 7 * * column 1, line 42 - line 52 * * column 3, line 13 - line 43 * -----	1-3,5,6, 11-13, 15,16, 21-23, 27-29, 31, 33-36, 38,39, 43-46, 48,49	G06F1/00
X	EP 0 715 244 A (XEROX CORP) 5 June 1996 (1996-06-05) * page 3, line 44 - page 6, line 36 * -----	1-4, 7-14, 17-37, 40-47, 50-52	
X	WO 99/63443 A (DATAMARK TECHNOLOGIES PTE LTD ; HO ANTHONY TUNG SHUEN (SG); TAM SIU CH) 9 December 1999 (1999-12-09) * page 7, line 10 - page 8, line 12 * * page 12, line 1 - line 8 * -----	1,4-6, 14-16, 24,30, 37-39, 47,49	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F
X	US 4 972 471 A (DALE JAMES ET AL) 20 November 1990 (1990-11-20) * abstract * * column 1, line 47 - column 2, line 33 * -----	1,5,6, 15,16, 38,39, 48,49	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	1 June 2004	Anticoli, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 0144

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-06-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5893067 A	06-04-1999	AU 3313397 A	25-02-1998
		JP 2002505758 T	19-02-2002
		WO 9806195 A1	12-02-1998
EP 0715244 A	05-06-1996	US 5715403 A	03-02-1998
		DE 69530658 D1	12-06-2003
		DE 69530658 T2	27-11-2003
		EP 1293865 A2	19-03-2003
		EP 1293866 A2	19-03-2003
		EP 1298516 A2	02-04-2003
		EP 1329791 A1	23-07-2003
		EP 1329792 A1	23-07-2003
		EP 1329793 A1	23-07-2003
		EP 1335264 A1	13-08-2003
		EP 1329794 A1	23-07-2003
		EP 0715244 A1	05-06-1996
		JP 8263440 A	11-10-1996
		JP 2003216764 A	31-07-2003
		JP 2003202932 A	18-07-2003
WO 9963443 A	09-12-1999	WO 9963443 A1	09-12-1999
		AU 7683398 A	20-12-1999
		EP 1103026 A1	30-05-2001
		JP 2002517920 T	18-06-2002
		TW 468344 B	11-12-2001
US 4972471 A	20-11-1990	CA 2088780 A1	15-03-1992
		WO 9205550 A1	02-04-1992
		EP 0548071 A1	30-06-1993
		JP 6500658 T	20-01-1994

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82